NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Report to the Secretary
of the U.S. Department of Health and Human Services

on

Enhanced Protections for Uses of Health Data:
A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data

October 21, 2007

Table of Contents

Introduction

Purpose and Scope

The Office of the National Coordinator for Health Information Technology (ONC) asked the National Committee on Vital and Health Statistics (NCVHS) to develop a conceptual and policy framework to balance the benefits, sensitivities, obligations, and protections of what has typically been referred to as secondary uses of health data. The need for enhanced protections for uses of health data increases in importance as health care moves from paper to electronic and from point-to-point data exchange to the vision of a nationwide health information network (NHIN).

NCVHS is proposing these recommendations to the Secretary of Health and Human Services (HHS) to advance the Nation's health and healthcare delivery system. Enhanced and more widely adopted data stewardship principles and other measures are needed to enable optimal uses of health data, while respecting the privacy of the individuals who are the sources of those data. Particular emphasis is placed on the immediate need to ensure that appropriate protections surround uses of health data for quality measurement, reporting, and improvement.

Secondary Uses of Health Data

In addressing the ONC request, NCVHS identified concerns with the term *secondary use.* Secondary use of health data has no standard reference. For example, some consider primary uses those for direct care and all other uses secondary. Others consider uses of health data for payment and healthcare operations also a primary use. In addition, grouping various uses of health data under the rubric of secondary use may result in treating all uses within that class the same. Different approaches may be needed to afford protections for different types of uses. Finally, the term secondary use carries the connotation that these uses of health data are less important than other uses. As a result, NCVHS does not use the term *secondary* to describe categories of uses. Instead NCVHS urges that the term be abandoned in favor of explicit description of each use of health data.

Information Analysis and Organization of Report

This report includes:

1. **Background** – This section describes the process NCVHS undertook to hear testimony and obtain input on the current state and issues related to uses of health data that form the basis for the recommendations.

2. **Current landscape** – This section summarizes the testimony concerning the current state of health data uses and identifies significant gaps in protections for

these uses which may be amplified as health information technology (HIT) and health information exchange (HIE) become more prevalent.

3. **Observations and recommendations** – This section provides observations and recommendations described within a framework of data stewardship. Initial focus is on practical solutions that can be implemented today to address overall gaps in accountability, transparency, individual participation and control, de-identification, security safeguards and controls, and data integrity and quality. Specific attention is also paid to recommendations for uses of health data that are most immediately enhanced through HIT and HIE – quality measurement, reporting, and improvement and research. There are also recommendations for evaluation of approaches suitable to protect other and potentially unanticipated uses as the transition is made to a NHIN. Finally, recommendations that may take longer to implement are made for comprehensive privacy and anti-discrimination legislation.

4. A **Taxonomy and Glossary of Terms** in **Appendix C** defines terms used throughout this report and underscores the broader need for standardization of terms describing various data stewardship approaches. For example, the terms *de-identification*, *anonymization*, and *pseudonymization* are all associated with protecting identity, but may be applied differently in different contexts, some of which diverge from the implementation specification of de-identification or limited data set according to the HIPAA Privacy Rule (§164.514(a), (b), (c), and (e)), herein referred to as *HIPAA de-identification*.

Report Background

NCVHS Coverage of Topic

NCVHS has a long history of engaging public comment, analyzing issues, and making recommendations to the Secretary of HHS on uses of health data from multiple perspectives. In 1996, Public Law 104-191, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, directed the NCVHS to be responsible generally for advising the Secretary of HHS and the Congress on the status of the implementation of the HIPAA Administrative Simplification provisions. Subsequently, NCVHS has issued annual reports on various HIPAA compliance issues. Public Law 104-191 also directed the NCVHS to "study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information," which generated several sets of recommendations. NCVHS has been at the forefront of promoting HIT and HIE. In 2001, NCVHS generated a report on Information for Health: A Strategy for Building the National Health Information Infrastructure, specifically addressing the need for a private, secure, and effective NHIN. Recommendations on the Initial Functional Requirements for a NHIN were delivered to the Secretary on October 30, 2006. Privacy issues within a NHIN were addressed in the NCVHS June

22, 2006 letter report entitled, Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network. An update to the Privacy Letter with respect to coverage of healthcare and other entities was delivered to the Secretary on June 21, 2007. The NCVHS Report and Recommendations on Personal Health Records and Personal Health Record Systems from February 2006 and its Letter Report to the Secretary on Personal Health Record (PHR) Systems from September 9, 2005, describe the state of affairs with respect to such health data collection.

NCVHS has also delivered numerous reports describing uses of health data for population studies and for use in quality improvement. Its Recommendations on Populations Based Data Collection, delivered to the Secretary of HHS on August 23, 2004, and its Report on Measuring Health Care Quality in May 2004 are seminal works on key issues for using health data. The Recommendation Letter on Data Linkages to Improve Health Outcomes on June 21, 2007 also addressed the special issue of merging data from disparate sources.

The NCVHS Web site (http://ncvhs.hhs.gov) provides access to all NCVHS documents referenced, as well as others.

NCVHS Process

To enable NCVHS to make practical recommendations to facilitate uses and exchange of health data for advancing the quality of the Nation's health and healthcare delivery system, the Committee's ad hoc work group (see **Appendix A** for list of members) received significant public comment, both in formal testimony as well as in open public sessions to discuss findings and provide input into recommendations.

Testimony

Testimony was taken on the Agency for Healthcare Research and Quality (AHRQ) request for information on data stewardship during its Committee meeting on June 21, 2007. NCVHS held three sets of hearings and open meetings in the Washington, DC area on July 17-19, August 2-3, and October 4-5, 2007. It published a pre-decisional draft document on its web site on October 19, 2007, and held an open call for public comment on October 31, 2007. It received several written comments from experts unable to attend these hearings. In drafting this report, NCVHS presented interim findings to the American Health Information Community Consumer Empowerment Work Group, September 12, Quality Work Group, October 3, and public meeting in Chicago on November 13, 2007.

In all, there were 58 testifiers from provider and consumer representatives, quality organizations, health information exchanges, vendors that process and use health data in a variety of ways, and the research and public health communities. (Testifiers are listed in **Appendix B**.) Members of the NCVHS also participated in the conference on

Toward a National Framework for the Secondary Use of Health Data sponsored by the American Medical Informatics Association (AMIA), June 14-15, 2007.

Although time for input was very short, NCVHS is appreciative of the effort so many put into contributing comments.

Current Landscape

NCVHS heard testimony that the common good for all Americans is served when health data can be used to advance the quality of health and health care for the Nation. There is optimism for the growing number of benefits that can be achieved through uses of health data enabled by health information technology (HIT) and health information exchange (HIE). NCVHS, however, also heard concerns surrounding potential harms that may arise from enhanced uses of HIT and HIE. Current regulations may not fully address the concerns that arise from the new uses of health data enabled by HIT and HIE. There is a growing need for enhanced and more widely adopted data stewardship principles and other measures to protect privacy.

Benefits from Enhanced Uses of HIT and HIE

At the point of care, HIT enhances access to information, affords patient safety alerts and health maintenance reminders, and supports care management. Across the continuum of care, HIE enables readily accessible information needed in an emergency, and more complete information and coordination of care among referring providers and for transfer of care, such as from a hospital to a long term care facility.

For quality measurement, reporting, and improvement, fully automated data collection processes provide for more efficient access to more comprehensive databases for benchmarking, as well as identification of new opportunities for improvement in care delivery. The ability to mine more comprehensive databases makes knowledge discovery more readily available for continuous quality improvement. HIE technologies that enable virtual aggregation of data and enhanced data linkage, such as individual person matching algorithms, support longitudinal data collection to improve future care of an individual and quality outcomes analysis. Testifiers also described improved and developing techniques available to secure data and to attach consent for use to the data.

Clinical and population research can be strengthened. Identification and participation of candidates for clinical trials across a larger geographic area enables more comprehensive cohorts for testing hypotheses. Health services and other population-based research is aided through the availability of large databases. As a result, hypotheses can be tested or complications detected more rapidly.

Disease control and prevention can be more accurate, complete, and rapidly accessible when new sources of data, fully automated data collection processes, and improved data linkage capabilities exist.

Concerns about the Potential for Harm Raised by HIT and HIE

Erosion of trust in the healthcare system may occur when there is a divergence between what the individual reasonably expects health data to be used for and when uses are made for other purposes without the knowledge and permission of the individual. Individuals who are the recipients of the care process appear to have a high degree of trust in their providers. There also appears to be a high degree of trust in public health from the perspective of protecting against disease outbreaks; and in health research when accompanied by informed consent. Trust erodes and privacy concerns may increase, however, when uses of health data are made for other less widely recognized purposes. In addition, when health data are sold – even when used to ensure the sustainability of the business model for enhanced uses of HIT or when the data are de-identified – there are heightened concerns.

Compromises to health care may result when individuals fail to seek treatment or choose to withhold information that could impact decisions about treatment because they do not understand how their data may be used, or they may distrust the ability of their identity to be protected, particularly when they consider the information especially sensitive. HIT can afford greater protections, but these must be diligently applied and made known to individuals.

Discrimination and personal embarrassment may be amplified as there is enhanced ability to automate health data collection, compile longitudinal data, re-identify data that have been de-identified, and to share data through HIE. There have long been legitimate concerns that personal health information is used in making decisions that adversely affect the individual, such as in employment, benefits coverage, or acceptance for loans or mortgages.

Need for Additional Clarity in HIPAA Privacy and Security Rules

Public Law 104-191 called for federal privacy legislation that ideally would have extended privacy requirements to all entrusted with personal health information. Without such legislation, however, the HIPAA Privacy and Security Rules cover only health care payers, clearinghouses, and providers who electronically transmit financial and administrative transactions (i.e., covered entities), and by contract the business associates of covered entities. Testimony to NCVHS describes several areas of omissions in the HIPAA Privacy and Security Rules as the transition is made to HIE,

and confusion among covered entities on how to carry out some of the requirements in light of new uses of health data enabled by HIT and HIE.[1]

Covered entities are held accountable for protecting individually identifiable health information which they maintain and/or transmit to others – described in HIPAA as *protected health information* (PHI). Covered entities do not include organizations and their agents who may also perform functions involving protected health information on behalf of a covered entity. As such, the HIPAA Privacy and Security Rules require these organizations to have business associate contracts or other arrangements with covered entities to apply the protections afforded by these Rules. The intent is to establish a chain of trust from the covered entity to the business associate and beyond. A particular challenge is that the farther removed the use is from the covered entity, the weaker is the ability to monitor the intent of the contractual obligations of health data protection.

Another challenge is that the HIPAA Privacy Rule only addresses identifiable protected health information. Once protected health information is de-identified according to the HIPAA definition of de-identification, it falls outside of the jurisdiction of the HIPAA Privacy and Security Rules. There is neither accountability nor transparency back to either the covered entity or the individual concerning use of these HIPAA de-identified data.

Finally, a growing number of uses of identifiable *personal health information* (i.e., individually identifiable health information not maintained or transmitted by a covered entity) fall outside of the HIPAA chain of trust (or other regulations, such as those over research on human subjects). An example is when individuals supply personal health information to personal health record (PHR) web sites not sponsored by covered entities or business associates. There will be increasing challenges with respect to HIPAA and chain of trust as hybrid PHRs, in which both covered entity-supplied and individual-supplied health data are collected, become more widely used.

Increasing Role of Health Data Stewardship

There is an increasing need to adopt enhanced data stewardship principles by all entities that have access to health data, independent of HIPAA covered entity status. When an individual provides personal health information to anyone else, in any manner (e.g., in person or online), the information is provided in confidence and with implicit trust that the information will not be used in unintended ways. The American Medical Informatics Association (AMIA) states that data stewardship "encompasses the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information." Further, AMIA notes that "principles of data stewardship apply to all the personnel,

[1] Linda Dimitropoulos, PhD, RTI International; William J. O'Byrne, New Jersey e-HIT; and Steve Posnack, ONC, Testimony on the Health Information Security and Privacy Collaboration (HISPC) Report of June 30, 2007, July 17, 2007

systems, and processes engaging in health information storage and exchange within and across organizations."

Views concerning a national health data stewardship entity have been sought by the Agency for Healthcare Research and Quality (AHRQ), based on principles recommended by AQA for performance of clinician-level quality measurement. An RFI issued on June 4, 2007 requested information about creating a "public/private entity that will set uniform operating rules and standards for sharing and aggregating public and private sector data on quality and efficiency; offer guidance on implementation of such national operating rules and standards; and provide a framework for collecting, aggregating, and analyzing data, to afford means of more effective oversight of healthcare data analyses and reporting in the United States." Although the need to create a data stewardship entity is outside the scope of the recommendations in this report, early responses were important to understand. A dichotomy was observed: Some respondents interpreted that a data stewardship entity would serve, itself, as database and to which respondents were highly adverse. Other respondents indicated that an entity that would provide guiding principles for good stewardship was very much needed, but would need to be a pristine and completely neutral body if put in the position of arbitrating good stewardship.[2]

NCVHS heard that when *any* organization that is responsible for making use of personal health information, i.e., when serving as a data steward, is trusted, there is greater acceptance of the use of the health data. This is the case independent of HIPAA covered entity status. Trust was observed to be something that an organization earned over time through acting as a responsible data steward. Trust may be enhanced through transparency and affording appropriate rights to individuals on how their health data may be used.

> *For example, the Northern New England Cardiovascular Disease Study Group has a comprehensive approach to providing (HIPAA quality assessment and research institutional review board) oversight for the collection of data, reporting outcomes, providing services to clinicians and institutions, and engaging individuals in their cardiac surgery decision making, such as through "prediction pocket cards" used to predict surgical risk, but which also serves as a good setting for informed consent. As a result of the many efforts taken to ensure transparency, there is a spirit of trust among clinicians, even across competing settings, and by individuals who have a clear picture of how their health data are used.*

NCVHS observes that the HIPAA Privacy Rule, despite being broad in definition and not anticipating every future use, provides an initial set of data stewardship principles for uses of health data. As new uses of health data are made in a new world of HIT and HIE, these principles need review and enhancement. Improving data stewardship is an important premise for building transparency and trust throughout all entities that may

[2] National Health Data Stewardship, Request for Information, Agency for Healthcare Research and Quality, *Federal Register*, Vol. 72, No. 106, Monday, June 4, 2007.

use health data for any purpose; and in particular to ensure that individuals are informed about uses of their health data which they may not anticipate.

However, it was also observed that transparency and trust have limits to their effectiveness and should not be substitutes for other measures. For example, the HIPAA notice of privacy practices (NPP) is a means to provide transparency, but does not achieve its purpose if it is not read or understood by individuals. Clarifying the language of a NPP or taking time to explain its contents, while beneficial, will not fully address trust issues.

A Health Data Stewardship Framework may aid potential users contemplating a specific use of health data to analyze the use and determine appropriate data stewardship approaches. In general, a framework is a conceptual structure used to solve a complex issue or outline possible courses of action. Achieving the benefits of health data uses while reducing the potential for harms presents a complex issue among a myriad of uses and users of health data. No single work can identify all uses and users, let alone anticipate all potential new uses and users. The Health Data Stewardship Framework depicted below builds upon the Taxonomy of the American Medical Informatics Association (AMIA); Connecting for Health Common Framework Privacy Principles from the Markle Foundation; and the cancer Biomedical Informatics Grid (caBIG™) Framework for Data Sharing Terms and Conditions.

Health Data Stewardship Framework

<table>
<tr><th colspan="7">Existing Data Stewardship Factors</th></tr>
<tr><td colspan="7">User status with respect to Federal/State legal/regulatory requirements (e.g., HIPAA covered entity or business associate, public health or other organization permitted personal health data by law, researcher covered by regulation, organization covered by FTC, other, none):</td></tr>
<tr><td colspan="7">Status of data (e.g., protected health information, HIPAA de-identified health data, personal health information):</td></tr>
<tr><th colspan="7">Benefit/Risk Analysis of Intended Use</th></tr>
<tr><td colspan="7">Intended use of data:</td></tr>
<tr><td colspan="3">Individual & Societal Benefits
from Intended Use of Data:</td><td colspan="4">Potential Risk for Harms
from Intended Use of the Data:</td></tr>
<tr><th colspan="7">Data Stewardship Approaches</th></tr>
<tr><td>Accountability/ Chain of Trust</td><td>Transparency</td><td>Individual Participation & Control</td><td>HIPAA De-identification</td><td>Security Safeguards & Controls</td><td>Oversight of Data Uses</td><td>Data Integrity & Quality</td></tr>
</table>

Specific Uses of Health Data

Uses of Health Data for Treatment, Payment, and Healthcare Operations

The HIPAA Privacy Rule permits covered entities to use and disclose protected health information without authorization from the individual when providing access to the individual; for treatment, payment, and healthcare operations (TPO); incident to an otherwise permitted or required use or disclosure, provided the covered entity has taken adequate safeguards; and when required by law, public health, and for certain other uses within prescribed limitations.[3, 4] (State laws which are more stringent may require authorization for some uses or disclosures.)

- *Treatment* means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to an individual; or the referral of an individual for health care from one provider to another.

- *Payment* refers to the activities undertaken by a health plan to determine coverage and provision of benefits under the plan and to obtain or provide reimbursement for the provision of health care.

- *Healthcare operations* encompass quality assessment, competency review, health benefits processes, compliance activities, business planning, and general administrative activities.[5]

A common theme that NCVHS heard in testimony related to the broad scope of some aspects of the HIPAA Privacy and Security Rules. Testifiers observed that HIPAA may serve well enough in providing data stewardship guidance for the "treatment and payment" processes of care delivery, but the area of "healthcare operations" was observed to be broad in scope and not well-understood by individuals. It was noted that trust may factor more heavily than laws and regulations with respect to individuals and their privacy concerns. The further a use of health data is from the point of care, the less transparency there may be and the less individuals may trust the ability of their health data to be protected.

Uses of Health Data for Quality Measurement, Reporting, and Improvement

The definition of quality assessment and improvement activities, included in the HIPAA Privacy Rule under healthcare operations, includes "outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable

[3] HIPAA Privacy Rule, §164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.
[4] HIPAA Privacy Rule, §164.514 Other requirements relating to uses and disclosures of protected health information (e) Limited data set, (f) Fundraising, and (g) Underwriting and related purposes.
[5] HIPAA Privacy Rule, §164.501 Definitions.

knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment" (§164.501).

Benefits of quality measurement and reporting include "better safety, effectiveness, patient-centeredness, timeliness, efficiency, and equity"[6] – the six aims for quality improvement specified in the IOM *Quality Chasm* report. Individuals can make more informed decisions about their care when quality is accurately reported. Providers can improve the quality of care delivered when they understand the current status of the care being provided and have access to evidence-based protocols. Payers can assure greater value through pay for quality and other mechanisms. Purchasers of care can ensure they are receiving value when they have access to accurate quality reporting.

Challenges in uses of health data for quality measurement, reporting, and improvement include that uses of health data for quality improvement are not well-known or understood by individuals. Furthermore, linking health data about individuals longitudinally, across multiple settings, and from multiple sources must be accurate to ensure meaningful outcomes, and must protect privacy. If an organization chooses to enhance protection of the health data by applying various forms of identity protection, such as pseudonymization, it should be aware that the increased amount of detailed person-level information available makes it more likely that some individuals could be identified. A burdensome process of identity protection, however, can result in not performing the linking, and not achieving the benefits anticipated.

Organizations that link health data have an important place in promoting quality health care but must not violate the trust of individuals and providers. For example, pharmacy benefits managers (PBMs), that may be covered entities or business associates, compiled medication histories for individuals impacted by the hurricane disasters of 2005 and provided an important public service. Today, such medication histories are being used to support medication reconciliation activities in compliance with The Joint Commission standards across provider settings. However, there are organizations who acquire health data by direct access through the systems they sell to HIPAA covered entities or by buying HIPAA de-identified data. Some of these organizations use the data to support quality purposes; but others may link the data to provider databases to market to providers, or use the data to target marketing to a circumscribed population likely to include a target group of individuals.

Uses of Health Data in Research

Variation in research regulations across different federal entities was also identified by testifiers as being potentially problematic. How health data may be used in research

[6] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century,* Washington, DC: National Academies Press, 2001, p. 43

varies among the HIPAA Privacy Rule, the Federal Policy for Protection of Human Subjects (45 CFR 46, a.k.a. The Common Rule), the Food and Drug Administration (FDA) Protection of Human Subjects Regulations (21 CFR 50 and 56), and the Protection of Human Subjects of Research in the Veterans Health Administration (VA) Regulations (38 CFR 16). The result can be confusion on the part of both individuals and researchers**.** An example cited was where an individual may be asked to participate in a research project sponsored by the VA and another project under the FDA jurisdiction, each with somewhat different requirements that may result in confusion about the two projects' needs for privacy protections.

Using data collected for quality improvement that evolves into a research study may violate the HIPAA Privacy Rule, and yet be of profound importance to the health of the Nation. A quality assessment study is defined under the HIPAA Privacy Rule as healthcare operations and does not require an authorization from the individual. However, use of protected health information for research either requires an authorization or a wavier of authorization from a privacy board, or an Institutional Review Board (IRB) when research is supported by federal funds. As value-based purchasing increases in prevalence and providers want to understand their own data better, the likelihood of compiling more comprehensive databases for immediate quality measurement and improvement increases. Such work initiated as part of performance improvement increasingly results in interesting, reportable findings that can improve quality of care for a larger population. How to distinguish a quality activity from a research study, and how to evolve the use of the data from quality into research, were issues cited by both provider and payer testifiers.

Uses of Health Data for Public Health

Public health databases are used for surveillance and to compile registries, such as in support of cancer treatment and to track immunization. Such uses are authorized by state and local law, and permitted under HIPAA. Yet surveillance is extending in scope, such as to collect Hemoglobin A1c values with the intent to contact individuals directly about potential improvements in diabetes management (e.g., New York). Testimony indicated that the transparency of such uses is variable. Most individuals are unaware of required reporting; others are aware to the extent that they may see a caregiver under a false name to avoid consequences of reporting. Public health data collected directly by the Centers for Disease Control and Prevention (CDC) are obtained using a variety of mechanisms. Included are health statistical data obtained from surveys, which may be conducted under an IRB process or with the consent of the individual responding to the survey. These data may be released to others only through strict data release agreements or as statistically de-identified datasets. CDC is starting nationwide data collection efforts, such as BioSense, that involve contractual agreements similar to HIPAA business associate contracts. Such efforts utilize new data sources and are enabled by fully automated data collection processes and enhanced data linkage capabilities. However, and despite new and better techniques to protect data, such large databases may present unanticipated issues or concerns for public health activities.

Increasing Concerns over Sale of Health Data

An increasing concern surrounding uses of health data is that relating to the sale of health data where financial benefit accrues to other than the individual who is the source of the data. HIPAA requires an authorization for any use by covered entities of protected health information for marketing except if the communication is face-to-face by the covered entity to an individual or if it is in the form of a promotional gift of nominal value provided by the covered entity (§164.508(a)(3)(i)). HIPAA also specifies that if marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved (§164.508(a)(3)(ii)).

There are not these same protections for organizations who may de-identify protected health information and sell it, or that are outside of HIPAA covered entity status that may collect identifiable personal health information. There is certainly a need for sustainable business models for research and development of HIT, for HIE and a NHIN to serve the public good, for personal health records, and other such purposes. However, when the uses are unknown or unanticipated by the individual, a lack of trust arises and the potential for resultant harms to the individual and society increase.

> *Example: An individual may benefit from a provider using an EHR. In turn, the provider may be able to afford the individual that benefit through using an EHR that is subsidized through the use of advertising. But when the EHR vendor mines the data to supply the advertising to the provider, or to sell directly to the individual, or to sell information to a third party for other uses, the individual's trust in the provider erodes and concerns about privacy increase.*

Observations and Recommendations

Currently, the health industry relies upon the HIPAA construct of covered entities and business associates to protect health data. The following observations and recommendations call for a transformation, in which the focus is on enhanced protections for all uses of health data by all users, independent of whether an organization is covered under HIPAA. NCVHS believes that data stewardship principles should be applied to all organizations that have access to personal health data. Data stewardship includes: accountability, transparency, individual participation and control, de-identification, security safeguards and controls, oversight of data uses, and data integrity and quality measures. The recommendations, however, also recognize the circumstances under which data stewardship principles apply and where there may need to be other actions.

HHS has a variety of means to achieve enhanced protections for uses of health data. These include issuance of guidance, such as the HIPAA Security Guidance

distributed by CMS on December 28, 2006; requirements for Federal agency adoption; inclusion of requirements in contractor rules; through incentives; in Conditions of Participation rules; and other processes in addition to recommending new legislation and issuing new regulations. The recommendations that follow urge adoption by whatever means is most expeditious and will promote the broadest possible adoption, including those which will most influence organizations not covered by HIPAA.

NCVHS commits to monitoring the usefulness of this guidance and offering further recommendations as may be needed.

1. Observations and Recommendations on Principles of Data Stewardship for Accountability and Chain of Trust within HIPAA

HIPAA Covered Entities

The HIPAA Privacy and Security Rules only apply directly to health care payers, clearinghouses, and providers who electronically transmit health information in connection with transactions for which HHS has standards. The protections afforded by the Privacy and Security Rules apply only indirectly to other organizations that may have access to protected health information when received by or on behalf of a covered entity.

Business Associates and Their Agents

The HIPAA Privacy and Security Rules permit covered entities to enter into a contract or other arrangement with organizations not covered under HIPAA but which support the work of the covered entity. The business associate contract must establish the permitted and required uses and disclosures of information by the business associate, and essentially binds the business associate to the data stewardship principles of the HIPAA Privacy and Security Rules. The covered entity may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate and to provide data aggregation services relating to the healthcare operations of the covered entity. The provisions in the HIPAA Privacy and Security Rules describe that the contract must be able to be terminated by the covered entity if there is a material breach or violation of the business associate's obligation under the contract. (§164.504(e) and §164.314(a))

In practice, an explicit enumeration of what data the business associate will use or how it intends to use the data is often not included in business associate contracts. Many business associate contracts are vague on what the business associate can do with protected health information. Consequently, this opens up an individual's data to uses that the individual does not anticipate and for which the individual may or may not be in agreement.

Business associate contracts require business associates to report "any use or disclosure of the information not provided for by its contract of which it becomes aware" (§164.504(e)(2)(ii)(c)). However, business associate contracts do not require periodic review or renewal. Since the description of permitted uses and disclosures is broad, the covered entity may be unaware of uses and disclosures the business associate is making of health data as these change over time.

> *For example, a business associate may collect data for the purpose of aggregating data for provider accreditation activities. The covered entity, however, may not be aware until after the fact that the business associate plans to set up a web site for public reporting of provider-specific reporting of chronic disease benchmarks.*

Business associates are also permitted to utilize agents in support of their work with covered entities. Business associates must ensure that any agents, including a subcontractor, to whom it provides protected health information . . . agrees to the same restrictions and conditions that apply to the business associate" (§164.504(e)(2)(ii)(D)), or in the case of the Security Rule "ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it ((§164.314(a)(2)(i)(B)). Business associates are not explicitly required to have a business associate contract with their agents that enumerate uses of data, and they are not required to identify the agents to the covered entity. As a result, there is no opportunity for the covered entity to monitor health data usage by agents of business associates.

> *For example, an EHR vendor that has a business associate contract with a covered entity may use a third party application service provider (ASP) to host the covered entity's EHR data at a remote location. The agent of the business associate, however, may de-identify the data and sell it to a health products supply company that links it to provider data and hence is able to target marketing to individuals in specific geographic regions, without the covered entity being aware of the use, object to the use, or describe such use to individuals it serves.*

Organizations Not Covered by HIPAA Privacy and Security Rules

Protections afforded by HIPAA only extend to covered entities and through contractual arrangements to their business associates the agents of the business associates. This leaves many organizations outside of the protections afforded by HIPAA:

- *Providers who do not file claims electronically* are not covered entities. NCVHS has learned that a number of providers are not covered by HIPAA, either because they do not submit electronic claims or receive payment directly from individual, or they are providers that create records covered by the Family Educational Rights and Privacy Act (FERPA) which are explicitly excluded from the definition of protected health information.[7]

[7] NCVHS Letter to the Secretary of HHS on Update to Privacy Laws and Regulations Required to Accommodate NHIN Data Sharing Practices, June 21, 2007

- *Companies providing data transmission services* who need to access the data being transmitted in order to conduct the transmission may or may not be business associates. If such transmissions are likened to an envelope, many of these companies only transmit data via routing information on the outside of the envelope. The response to a Frequently Asked Question (FAQ) posted on the HHS Office for Civil Rights (OCR) web site, observes that "the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information." A conduit is described as "an organization that transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation services or as required by law." The response to the FAQ goes on to note that "since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity."

  However, there are some companies who provide transmission services which do need access to the contents of the envelope. Examples might include e-prescribing gateways that may need to convert a prescription transaction from one version of the NCPDP standard to another, or from the electronic transaction to a fax. Banks are increasingly gaining access to explanations of benefits as they process electronic funds transfers. Some of these companies recognize themselves as business associates or are required by the covered entity with whom they do business to have business associate contracts. In other cases, however, the company may originally not have been a business associate, but over time the level of access may increase.

  > *For example, an e-prescribing gateway that only initially transmitted data between providers and pharmacies as a conduit may become a business associate when it is asked to follow a provider's specific routing instructions based on drug type for prescription refill requests.*

- *Personal health record services* that are not part of covered entities are increasing in number. Many, though not all, are offered via web sites. The Congress has not enacted any law requiring privacy policies on web sites, however, the Federal Trade Commission (FTC) has broad authority under the Federal Trade Commission Act to bring enforcement actions against those engaging in "unfair or deceptive acts or practices in or affecting commerce."[8] The FTC can use this authority to prosecute companies that mishandle consumers' personal information. An increasing number of states are following the lead of the California Online Privacy Protection Act (COPPA) that requires the operator of any web site that collects "personally identifiable information" from California residents to post a privacy policy. In California, violators are subject to an

[8] Privacy Policies Increasing in Importance, Willcox & Savage P.C., April 2006

injunction and/or a civil penalty of $2,500 for each infraction. Private actions can also be brought under this statute.

- *Other companies with no relationship to covered entities*, such as life insurers, employers, schools, and others, also collect individually identifiable health data and are not regulated by HIPAA. While individuals may voluntarily choose to participate in such data collection, therein providing an implicit consent for data collection, there are concerns as to whether individuals are aware of how the data may be used. As personal devices that collect health data and automatically transmit it electronically to web sites become more prevalent, concerns about how the data are used are increasing.

  For example, an employee posting health information to an employer wellness program web site may be unaware that the data are used by the employer to design insurance benefit packages.

1.1 **Recommendation on business associate contract provisions**: HHS should take applicable means to ensure that covered entities specify the limits of health data use in their business associate contracts. In addition, HHS should apply these means to limit uses of health data in their own contracts. Covered entities should specify in their business associate contracts:

1.1.1 **terms that explicitly limit what identifiable health data may be used and for what purposes, by both the business associate and by any agents with whom the business associate may contract.** This allows the covered entity to describe such uses to individuals and monitor any potential changes over time.

1.1.2 **terms that specifically limit what uses may be made of HIPAA de-identified data and to whom HIPAA de-identified data are supplied.** This allows the covered entity to describe such uses to individuals and monitor any potential changes over time.

1.1.3 **that there must exist a contract or other agreement, equivalent to the business associate contract as described above, between the business associate and all of its agents**, including agents of agents. This assures a chain of trust from the covered entity through all organizations that may have access to identifiable or HIPAA de-identified health data. It also enables the covered entity to be able to describe uses of health data made by agents to individuals and monitor any potential changes over time.

1.1.4 **that any organization that specifies it will use de-identified data at the individual person-level for a specified purpose will ensure that the de-identification process follows the HIPAA requirements for de-identification**.

1.2 **Recommendation on attestation of business associate contract compliance**: HHS should take applicable means, such as issuing guidance and incorporating in their own requirements, to ensure that covered entities use an attestation process which includes that (a) business associates must provide an annual attestation to the covered entity that their actions remain consistent with the permitted uses, (b) all agents have been properly engaged by the business associates, and (c) the business associate and its agents are in compliance with all other applicable provisions of the business associate contract. In the event of any changes in uses or agents, the business associate contract must be amended.

1.3 **Recommendation on entities providing data transmission functions**: HHS should provide guidance that clarifies that any company providing data transmission of protected health information and who requires access to the protected health information in order to conduct the transmission is a business associate and must be bound by the requirements for business associates. This does not apply to routing instructions external to the protected health information content of the transmission.

1.4 **Recommendation on FTC privacy policy support**: HHS should urge the Federal Trade Commission (FTC) to utilize their full authority to ensure that (1.) privacy policies on web sites collecting personal health information fully inform users of the uses that will be made of their personal health information and (2.) the companies do not engage in misleading advertising or other deceptive trade practices. Further, when more inclusive Federal privacy legislation may be enacted, these web sites must be included. HHS should then collaborate with the FTC to promote harmonization of regulations covering these organizations to ensure consistent privacy protection.

2. Observations and Recommendations on Principles of Data Stewardship for Transparency

The primary means by which HIPAA covered entities provide transparency today is through distribution of a notice of privacy practices (NPP), which is intended to explain to individuals how their protected health information may be used and disclosed. Providers who have a direct treatment relationship with an individual must make a good faith effort to have the individual acknowledge receipt of the NPP. As a result, the NPP is often referenced as a “HIPAA consent,” when it is only an informational document advising individuals about the covered entity’s information policies and procedures. In addition, the NPP is frequently long, difficult to read, and is only required to provide examples of uses and disclosures. A NPP is not required to describe potential uses of de-identified data.

Related to the NPP, the HIPAA Privacy Rule provides a series of privacy rights, including the right to request privacy protection by means of a restriction or confidential

communications, right of access, right to amend, and right to an accounting of disclosures. All of these rights have some limitations which the covered entity may apply to protect the health information that serves as its business records. For example, individuals may be denied the ability to amend information not created by the covered entity, yet if this information carries erroneous information that has led to medical identity theft, the information may be perpetuated in other organizations' information systems.

Because of the limitations inherent in the NPP and its rights, and the extensive network of business associates and their agents that many covered entities use, the NPP is not serving well in alerting individuals to all potential uses of their health data or clarity surrounding how they may exercise control over uses of their health data. NCVHS heard testimony about several projects focusing on the need for transparency in communication about personal information. Findings from these projects revealed a number of insights:

> *For example, in a consumer research project for developing privacy notices performed for six federal agencies, it was found that the point of a disclosure form is not to lead people to a conclusion or particular action, but to give them information to make an informed decision – based on their own values*.[9]
>
> *Another example from a risk communication specialist discussed advice for medical institutions concerning concerns about misunderstanding or misuse of information released to persons or the public, indicating that the remedy for misunderstanding is always more information, not less*.[10]
>
> *A "lay person's" perspective observed that most individuals do not know about the use of their personal health information; that physicians are often worried about these uses; and that transparency would lead to investment in increasing involvement and engagement by individuals in their health care*.[11]

2.1 **Recommendation on Transparency**: HHS should issue guidance to covered entities and all other organizations responsible for managing, collecting, viewing, storing, sharing, disclosing, or otherwise making use of personal health information, whether identified or de-identified, to ensure that individuals have the opportunity to be informed about all potential uses of their health data that might not reasonably be anticipated to flow from the individual's disclosure of health information. Transparency should be achieved through:

2.1.1 **enhancements to the NPP**: HHS should issue guidance to covered entities on enhancing the HIPAA notice of privacy practices (NPP) to clarify uses of health data and to make the acknowledgement of receipt a more meaningful process. As an initial step, HHS should issue guidance

[9] Susan Kleimann, PhD, Kleimann Communication Group, Inc., Testimony, August 23, 2007
[10] Peter M. Sandman, Written Testimony, August 8, 2007
[11] Sharon F. terry, Genetic Alliance, Testimony, August 2, 2007

on writing model notices in plain language and offer other tools to enhance understanding of the NPP.

2.1.2 **making information available about the specific uses and users of protected health information**: HHS should issue guidance to covered entities to incorporate reference in the NPP that information, updated annually via the business associate contract attestation process, about how protected health information is used by business associates and their agents is available on the covered entity's web site and upon request.

2.1.3 **making information available about the specific nature of protected health information disclosed to other organizations, such as public health**: HHS should issue guidance to covered entities to incorporate reference in the NPP that information about what protected health information is disclosed to other organizations, such as to public health, is available on the covered entity's web site and upon request.

2.1.4 **ensuring that there is the ability by the individual who is a victim of medical identity theft to have errors corrected**: HHS should issue guidance to covered entities that individuals should be permitted to correct errors relating to medical identity theft in information that is incorporated into their designated record set but that was not created by the covered entity. This assures that errors are not perpetuated and transmitted to others when such information may be disclosed to other treating providers as permitted by the HIPAA Privacy Rule.

2.2 **Recommendation for education on uses of health data**: HHS should develop and maintain a multi-faceted national education initiative that would enhance transparency regarding uses of health data in an understandable and culturally sensitive manner. The initiative should involve all relevant HHS agencies. Educational activities should be appropriately integrated into Federal agencies' respective programs, policies and practices, as well as directly targeted to public and professional audiences. Various educational modalities should be included in NHIN trial implementations and other federally-sponsored demonstrations.

3. Observations and Recommendations on Principles of Data Stewardship for Individual Participation and Control over Personal Health Data

The NCVHS Privacy Letter of June 22, 2006 observes that providers should have the right to maintain health data in any medium. It notes, however, that it may be appropriate to permit individuals to opt into or out of certain other uses of health data. For example, it may be suitable for individuals to opt out of direct disease management interventions by health plans. Testimony was heard from a health information exchange in which individuals were asked to opt into contributing data to a provide-oriented

outcomes analysis and benchmarking data warehouse. They found that a high percentage (94 percent) of individuals opted in, with variation by specialty of providers.[12]

Testifiers to the NCVHS were particularly concerned about uses of individuals' health data which would be unanticipated by the individual. When individuals perceive benefit to themselves, trust is greater than when there is no perceived benefit or when there is benefit that accrues solely to someone else.

Testimony also identified a number of new and innovative approaches to manage individual consent with respect to health data uses. These include health record banking models, consent metadata, and federated consent registries. While these processes are new and need testing, they may provide a suitable way for consent to follow data.

3.1 **Recommendation on obtaining consent for of identifiable personal health data**: HHS should take applicable means to assure that uses or disclosures of identifiable personal health information held by any organization not covered by HIPAA and that are outside of HIPAA permissible uses or disclosures must obtain an authorization from the individual. See also Recommendation 9.1.

3.2 **Recommendation on consent management**: HHS should include in its NHIN trial implementations and other federally-sponsored demonstrations the evaluation of various new technologies that afford the ability for individuals to exercise control over disclosures of their personal health information. The evaluation of consent management should include determining to what data sharing scenarios consent would provide optimal protection while assuring the benefits of health data uses.

4. Observations and Recommendations on Principles of Data Stewardship for De-Identification

The HIPAA Privacy Rule applies only to protected health information. Therefore, the Privacy Rule permits use of de-identified data without individual authorization. It permits either a safe harbor or statistical approach to de-identification. De-identification removes the data from the protection of HIPAA requirements. Uses of de-identified data by any organization are not required to be tracked in any way.

In addition, applications of HIPAA's safe harbor definition of de-identification often remove only the 17 data elements in the definition and ignore the requirement to remove "any other unique identifying number, characteristic, or code, except as permitted" (§164.514(b)(2)(i)(R)). One testifier indicated that removal of the 17 data elements specified in HIPAA may result in a small ability to re-identify an individual.[13]

[12] Micky Tripathi, PhD, MPP, Massachusetts eHealth Collaborative, Testimony, August 23, 2007.
[13] In testimony on August 23, 2007, Latanya Sweeney, PhD, Carnegie-Mellon University, described a 0.04% chance of re-identifying data when de-identified by removal of the 17 data elements in the HIPAA

Other forms of identity protection, such as anonymization, masking, etc. (see **Appendix C**: Taxonomy/ Glossary of Terms), have also been adopted by certain entities – whether to remove the data from the protection of HIPAA or to enhance the protection beyond what is required. For example, covered entities are permitted to disclose protected health information for public health purposes. Because public health departments are very sensitive to the data they hold, they may use an approach called pseudonymization to protect the identity of the data yet enable re-identification when authorized. Other organizations, however, may be using de-identification techniques that are not consistent with the HIPAA requirements and pose a risk to personal privacy.

Finally, use of HIPAA de-identified data may not only pose risk to individuals but to providers. For example, testimony from the Prescription Project raised concerns about potential conflicts of interest in the medical profession created by pharmaceutical marketing conducted through data-mining of physician prescribing records.

4.1 **Recommendation on de-identification**: HHS should issue guidance to covered entities that clarifies that the HIPAA definition of de-identification (by the complete safe harbor definition or statistical method) is the only permitted means to de-identify protected health information. Furthermore, HHS should issue guidance on the specific threshold of statistical de-identification that ensures information is rendered not individually identifiable.

4.2 **Recommendation on allowable uses of HIPAA de-identified data without authorization**: HHS should define allowable uses of HIPAA de-identified data, and provide guidance to covered entities regarding what uses of HIPAA de-identified data are not permitted without authorization by the individual so that covered entities may be guided in development of their business associate contracts. See also Recommendation 1.1.2.

4.3 **Recommendation on sale of de-identified data**: HHS should examine the issues surrounding sale of de-identified data and propose guidelines that address best data stewardship practices. NCVHS will conduct hearings to assist in determining how to structure these guidelines.

5. Observations and Recommendations on Principles of Data Stewardship for Security Safeguards and Controls

The HIPAA Privacy Rule describes implementation specifications for minimum necessary uses of protected health information, including the identification of persons or classes of persons in its workforce who need access to protected health information to carry out their duties, and for each person or class of persons the category or

---

safe harbor definition of de-identification when compared to voter registration records for a confined population.

categories of protected health information to which access is needed, and any conditions appropriate to such access (§164.514(d)(s)(A) and (B)).

The HIPAA Security Rule affords the administrative and technical safeguards to support minimum necessary uses and disclosures. Administrative safeguards include access authorization in which policies and procedures must describe how access to electronic protected health information may be granted, for example, to a workstation, transaction, program, process, or other mechanism (§164.308(a)(4)(ii)(B)). Technical safeguards require implementation of technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). This requirement for access controls includes emergency access procedures, commonly referred to in the industry as "break-the-glass" mechanisms that enable necessary access in an emergency, often accompanied by the means to quickly annotate a rationale for the access and with generation of a special audit trail.

Testifiers to NCVHS reported that utilization of such technology and others, such as digital signature using X.509 certificate and non-repudiation for person or entity authentication are technologies available and being used successfully in some implementations.[14] It was also observed that not all covered entities deploy such technology. For example, several hospitals recently adopted a "zero-tolerance policy" on confidentiality, including use of computer programs to identify suspicious cases, and found significant reduction in employees disciplined for privacy violations.[15]

5.1 **Recommendation on technical data security management approaches**: HHS should issue guidance to covered entities to promote use of technical security measures to reduce unauthorized access, and to ensure that their business associates and agents are fully compliant with the HIPAA Security Rule authorization, access, authentication, and audit control requirements.

6. Observations and Recommendations on Principles of Data Stewardship for Data Integrity and Quality

HIT and HIE can aid in comprehensive data collection and sharing, but data integrity, uniformity of definition, and validity must be assured. Just because data are available electronically, does not mean that the data are accurate or are reliably captured or processed. As enhanced uses of health data are enabled by the creation of larger, more comprehensive databases, with the potential for linkage of personal health information to acquire longitudinal views, data integrity and quality become essential for meaningful uses of the health data.

[14] Assaf Halevy, dbMotion, August 23, 2007

[15] Minnesota Facilities Target Unauthorized Employee EHR Access, *Minneapolis Star Tribune*, July 19, 2007.

For example, during hearings on NHIN functional requirements, NCVHS heard testimony describing the multiple ways Hemoglobin A1c may be referenced (e.g., Hb A1c, Hg A1c, A1C, GHb*) and the issues this causes in managing laboratory processes and reporting results.*

Furthermore, erroneous assumptions about accurate data may be made during aggregation resulting in misinformation.

For example, while it is important to know that everyone who is diabetic has had a Hemoglobin A1c measured; it is not accurate to assume that everyone having had a Hemoglobin A1c test is a diabetic.

6.1 **Recommendation on data integrity and quality:** HHS data stewardship guidance should include that data captured, aggregated, and analyzed for quality measurement, reporting, and improvement follow rules and guidelines that ensure the precision and reliability of quality measures. See NCVHS recommendations on quality September 26, 2007.

7. Observations and Recommendations on Oversight for Specific Uses of Health Data

Uses of Health Data for Quality Measurement, Reporting, and Improvement:

As identified in the HIPAA definition of quality assessment and improvement activities within healthcare operations, uses of health data for quality activities may be many and varied. The HIPAA Privacy Rule accounts for the fact that many such uses might not have been able to be anticipated at the time of the writing of the Rule. It allows for "related functions that do not include treatment" to be covered under the definition.

In addition, HIPAA defines an organized health care arrangement (OHCA) that supports the sharing of health data for quality assessment purposes. An OHCA is defined in HIPAA as a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; an organized system of health care in which more than one covered entity participates in utilization review, quality assessment, or payment activities; and various configurations of group health plans that share the same sponsor or participants (§160.103).

NCVHS was asked by ONC to consider whether there were or should be boundaries around what quality activities are included in HIPAA's definition of healthcare operations and which may be outside of that definition and may call for greater choice by individuals whose data are included.

Several testifiers observed that they had instituted oversight processes to ensure that quality assessment activities were, indeed, those described by HIPAA. Previously cited

was the Northern New England Cardiovascular Disease Study that might be described as an OHCA under HIPAA and provides regular quality assessment oversight.

Several recent articles also describe the state of affairs in quality improvement. O'Kane raises issues with traditional approaches to quality assurance. She observes that "most management structures do not support integrated quality management" that would enhance accountability for quality, and describes the need for a quality oversight process by a responsible structure accountable to senior management and the governance of the institution for all quality improvement activities. O'Kane further notes that oversight "will not only protect patients from ad hoc or poorly conceived QI projects, it will also ensure that the institution has a vigorous and strategic agenda to improve the quality of its care."[16] Dubler and others argue that "if the data are adequately protected to address issues of individual privacy, individual informed consent should, in general, not be required." They also observe that a process of "informed participation," which they define as a process in "which institutions design quality improvement interventions and educate and engage patients about their obligations to help improve quality" will "allow the vast majority of quality improvement projects to go forward without triggering [a research-like informed consent process]."[17]

7.1 **Recommendation on protecting data for quality measurement, reporting, and improvemen**t: HHS should issue guidance to covered entities that health data uses for quality measurement, reporting, and improvement:

7.1.1 **are within the scope of healthcare operations** when conducted by covered entities or their business associates, and under the accountability and data stewardship principles of HIPAA.

7.1.2 **when conducted across covered entities within an organized health care arrangement** as defined by HIPAA, are within the scope of the HIPAA definition of healthcare operations, although the covered entities should assess any heightened risk of potential harm to individuals through such use of HIE and take measures to further protect the data, such as through pseudonymization.

7.1.3 **should have a proactive oversight process** to ensure there is compliance with HIPAA in uses of health data for quality measurement, reporting, and improvement that would be accountable to senior management and the governance of the institution. Where it is determined through a risk/benefit analysis that there is heightened risk to individuals from the quality reporting process, the oversight process should recommend extra precautionary measures to protect the individuals.

[16] O'Kane, Margaret, "Do Patients Need to be Protected from Quality Improvement?" 2007.
[17] Dubler, Nancy, Jeffrey Blustein, Rohit Bhalla, David Bernard, "Informed Participation: An Alternative Ethical Process for Including Patients in Quality-Improvement Projects," 2007.

Uses of Health Data for Research

The Common Rule (45 CFR 46) defines research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." While federally funded research studies on human subjects requires approval by an institutional review board (IRB) and an informed consent to "opt in" to participating in the research project, NCVHS heard testimony that there is variation in regulations addressing human research protections across the HIPAA Privacy Rule, the Common Rule, the FDA regulations (21 CFR 50 and 56), and the VA regulations (38 CFR 16). In addition, the Common Rule does not apply to human subjects' research when not supported by federal funds, being conducted in contemplation of a submission to the Food and Drug Administration (FDA), or conducted by an institution that has signed a multiple program assurance with the Office for Human Research Protections (OHRP). Representatives from the OHRP indicated to NCVHS that work was being done on clarifying the elements contained in the definition of research and that there is a Trans-HHS Taskforce on Harmonization of Ethical and Legal Policies Related to the Use of Human Specimens and Data in Research (HELPS) composed of representatives from NIH, FDA, OCR, OHRP, CDC, and others focused on harmonizing regulations under the jurisdiction of HHS.

NCVHS heard from many testifiers that quality activities are sometimes difficult to distinguish from research, and that some quality activities may evolve into research studies. It was observed that the "line between quality improvement and clinical research is relatively permeable, and it is sometimes difficult to determine with precision whether a project should be considered quality improvement or research, especially when a quality study may utilize techniques of randomization and prospective intervention with the support of electronic databases."[18] Testimony to NCVHS described a full spectrum of how organizations addressed the quality/research conundrum, from requesting annual IRB review of quality studies to giving individuals the opportunity to opt-out of using their data in research studies conducting retrospective review of data.

Good quality improvement activities share important characteristics with research, especially with respect to their ethical underpinnings. Lumpkin observes that basic principles of biomedical ethics, including respect for autonomy, beneficence, non-maleficence, and justice relate to all aspects of HIPAA TPO, and equally in quality, public health, and research uses of health data.[19]

There are also important differences between quality and research. The University of Texas M. D. Anderson Cancer Center notes that working definitions of quality improvement and research and methods of supervising and providing ethical oversight for quality improvement projects, including posting descriptions on their web, have actually evolved the inherent value of quality improvement. At M. D. Anderson, organizational leaders and IRB chairs use an informal triage process to decide which

[18] E. Bellin and N.N. Dubler, "The Quality Improvement-Research Divide and the Need for External Oversight," *American Journal of Public Health*, 91(9)(2001): 1512-17.
[19] Lumpkin, John R., MD, MPH, Robert Wood Johnson Foundation, Testimony on August 1, 2007.

projects should be considered quality improvement and which should be considered research. The federal definition of research [45 CFR 46] is sometimes applied to quality improvement projects.[20]

Another group that has grappled with the distinction between research and quality is the Center for Health Studies at Group Health Cooperative (GHC) in Seattle. GHC observes that distinguishing between quality and research in some situations is very difficult, noting that "determining whether an analysis of health data is "systematic" or "generalizable," and therefore considered research, is complicated and subjective."[21] They also observe that researchers strive to work collaboratively. The result is often that confusing or ambiguous regulations are negotiated within an organization, where it would be helpful to have a recognized national resource that could provide authoritative answers to regulatory questions. GHC utilizes a decision tree framework to guide its internal activities in determining when an activity is not research, when there is overlap, and when an activity is research

7.2 **Recommendation on harmonizing research regulations**: HHS should promote harmonization of research regulations within HHS and with other Departments that oversee regulations on human research protections to ensure consistent privacy and human subject protection.

7.3 **Recommendation for quality/research guidance:** HHS should encourage the Office of Human Research Protections (OHRP) in compiling its clarifying work on the research definition to continue to work collaboratively with the Office of Civil Rights (OCR) and to leverage the tools starting to be used in the industry to aid in distinguishing how requirements apply to uses of health data for quality and research, especially as questions relating to distinctions between research and quality uses of health data under the HIPAA healthcare operations definition arise.

7.4 **Recommendation for wide dissemination of quality/research guidance:** HHS should encourage the Office of Human Research Protections (OHRP) in compiling its clarifying work on the definition of research to widely disseminate the results. Limiting such dissemination only to the research community can limit its usefulness for providers, payers, and others who may not consider themselves researchers, but who may become engaged in quality work that ultimately falls within the scope of research on human subjects.

7.5 **Recommendation for means to transition quality activities into research when appropriate**: HHS should support OHRP and OCR collaboration so that important findings from a quality study can be appropriately evolved nto research when appropriate and that the HIPAA Privacy Rule provisions for authorization or

[20] Holm, Margaret J., et al, "Quality Improvement or Research: Defining and Supervising QI at the University of Texas M. D. Anderson Cancer Center, 2007.
[21] Immanuel, Virginia, Karin Johnson, Barbara Young, Gene Hart, Center for Health Studies, Group Health Cooperative, Seattle, Written Testimony, July 31, 2007.

waiver of authorization by a Privacy Board or Institutional Review Board are not violated.

8. Observations and Recommendations on Transitioning to a NHIN

NCVHS observes that many uses of health data contemplated to be supported by a NHIN are being made today in the context of point-to-point communications, often between covered entities, their business associates and agents, and with individual recipients of care delivery services. At this time, a definition of a NHIN and how it will be used has not reached sufficient maturity to dictate how individual choice over uses of health data within a NHIN should or could be exercised.

8.1 **Recommendation on choice within a NHIN**: HHS should continue to pursue further definition of a NHIN and its uses, and concurrently study how to balance the benefits of health data uses as development of a NHIN progresses with the concerns expressed about potential for harms. Trial implementations and other federally-sponsored demonstrations should include:

8.1.1 **evaluation of how individual choice might best be applied**, including evaluation of the costs and benefits of educating individuals, explaining and offering consent options, and ensuring transparency.

8.1.2. **evaluation of enhanced oversight and data stewardship principles** on various uses of health data, especially as more comprehensive databases may be compiled by non-HIPAA covered entities spawned by a NHIN.

8.1.3 **evaluation of de-identification techniques** to determine their effectiveness to protect identity and not enable re-identification when not intended.

8.1.4 **evaluation of and continued maturity of chain of trust mechanisms** to determine the impact on business associate relationships and ensure transparency between covered entities and business associates and their agents.

8.1.5 **evaluation of educational modalities** to determine the most effective messages and media for various target audiences.

8.1.6 **evaluation of appropriate safeguards needed to ensure that there is no unintended harm to individuals as de-identified data may be sold to support** the possible business models of a NHIN.

8.1.7 **evaluation of guidance that may be issued for covered entities to use or disclose protected health information in the least identifiable form consistent with the intended use.**

8.2 **Recommendation on adopting functional requirements for a NHIN to support data stewardship**: HHS should require NHIN trial implementations and other federally-sponsored demonstrations to adopt the functional requirements described by the NCVHS in its report to the Secretary of October 30, 2006, especially with respect to certifying participants, as well as to ensure that the principles of good stewardship outlined in these recommendations are fully adopted.

9. Observations and Recommendations on Privacy Legislation

Testimony indicates that there is a continuum of users of health data – from those with a close nexus with the delivery of care for the individual (i.e., individual care recipients, providers, and payers) to those that are very far removed from the individual-provider-payer relationship (e.g., data mining companies that track health-related web sites). Testimony also identified that, while the HIPAA Privacy and Security regulations address protections as health data are used close to the nexus of care delivery, the farther removed from care delivery, the less protection, if any, is afforded. The lack of adequate protections across all uses of health data can result in serious harms to individuals and ultimately the quality of health and health care in the Nation.

NCVHS has previously made several sets of recommendations setting the broad context for privacy improvement, including that privacy and confidentiality rules should apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools.

Finally, there is the need to address variations in state laws with respect to privacy. While it is important to identify best practices and states may be in the best position to test various practices, disparate laws across states make it costly and difficult for covered entities to comply with all nuances of the laws when data are exchanged across state boundaries.

9.1 **Recommendation on federal privacy legislation**: HHS should work with other federal agencies and the Congress:

9.1.1 **for more inclusive, federal privacy legislation** so that all individuals and entities that use and disclose individually identifiable health information are covered by the data stewardship principles, including a range of entities not currently covered by HIPAA. NCVHS recommendations of June 22, 2006 reference that “privacy and confidentiality rules [should] apply to all

individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools." To clarify, commercial data providers should include commercial vendors of personal health record services.

9.1.2 **on expanding the definition of covered entity under HIPAA**: *In the absence of comprehensive privacy legislation,* HHS should advocate for more limited legislation that expands the definition of covered entity under HIPAA from its focus on financial and administrative transactions to cover any entity that manages, collects, views, stores, shares, discloses, or otherwise makes use of personal health information.

9.2 **Recommendation on anti-discrimination legislation/regulation**: HHS should work with other federal agencies and the Congress for legislative or regulatory measures designed to eliminate or reduce as much as possible the potential discriminatory effects of misuse of health data (see also NCVHS Privacy Letter, June 22, 2006). This includes strengthening laws making it illegal for employers to discriminate in hiring, promotion, discharge, or other terms and conditions of employment unless the individual, with or without reasonable accommodation, is unable to perform the essential functions of the job.

9.3 **Recommendation on state data restriction laws**: HHS should support the work of the Health Information Security and Privacy Collaboration (HISPC) that would guide harmonization among state laws where applicable and pinpoint where states have made explicit differences. HHS should support a state law mapping repository that clarifies where states differ and which aspects of state laws are more stringent than HIPAA.

Appendix A: NCVHS Members

CHAIR
Simon P. Cohn, M.D., M.P.H.
Associate Executive Director
The Permanente Federation
Kaiser Permanente
Oakland, California

HHS EXECUTIVE STAFF DIRECTOR
James Scanlon
Deputy Assistant Secretary
Office of Science and Data Policy
Office of the Assistant Secretary
for Planning and Evaluation, DHHS
Humphrey Building, Room 442-E
Washington, DC

EXECUTIVE SECRETARY
Marjorie S. Greenberg
Chief
Classifications and Public Health Data
Standards Staff
Office of the Director
National Center for Health Statistics, CDC
Hyattsville, MD

MEMBERSHIP

Jeffrey S. Blair, M.B.A.
Director of Health Informatics
Lovelace Clinic Foundation
Albuquerque, NM

Justine M. Carr, M.D.
Senior Director
Clinical Resource Management
Beth Israel Deaconess Medical Center
Boston, MA

Leslie Pickering Francis, J.D., Ph.D.
Chairman, Department of Philosophy
Alfred C. Emery Professor of Law
University of Utah
Salt Lake City, UT

Larry Green, M.D.
University of Colorado
Health Science Center
Aurora, CO

John P. Houston, J.D.
Vice President, Privacy & Information Security
Assistant Counsel & Adjunct Professor
Professor of Biomedical Informatics
University of Pittsburgh School of Medicine
Pittsburgh, PA
Term: 12/01/2006 - 12/01/2010

Garland Land, M.P.H.
Executive Director
National Association for Public Health
Statistics
and Information Systems
Silver Spring, MD

Carol J. McCall, F.S.A., M.A.A.A.
Vice President
Humana
Center for Health Metrics
Louisville , KY

J. Marc Overhage, M.D., Ph.D.
President and CEO
Indiana Health Information Exchange
Associate Professor, Indiana University
School of Medicine
Senior Research Scientist, Regenstrief

Institute
Regenstrief Institute, Inc.
Indianapolis, IN

Harry Reynolds
Vice President
Blue Cross Blue Shield of North Carolina
Durham, NC

Mark A. Rothstein, J.D.
Herbert F. Boehl Chair of Law and Medicine
Director, Institute for Bioethics, Health Policy and Law
University of Louisville School of Medicine
Louisville, KY

William J. Scanlon, Ph.D.
Health Policy R&D
Washington , DC

Donald M. Steinwachs, Ph.D.
Professor and Director
The Johns Hopkins University
Bloomberg School of Public Health
Department of Health Policy and Management
Health Services Research and Development Center
Baltimore, MD

C. Eugene Steuerle, Ph.D.
Senior Fellow
The Urban Institute
Washington, D.C.

Paul Tang, M.D.
Chief Medical Information Officer
Palo Alto Medical Foundation
Palo Alto, CA

Kevin C. Vigilante, M.D., M.P.H.
Principal
Booz-Allen & Hamilton
Rockville, MD

Judith Warren, Ph.D., RN
Associate Professor
School of Nursing
University of Kansas
Kansas City, KS

LIAISON REPRESENTATIVES

J. Michael Fitzmaurice, Ph.D.
Senior Science Advisor for Information Technology
Agency for Healthcare Research and Quality
Rockville, MD

Edward J. Sondik, Ph.D.
Director
National Center for Health Statistics
Hyattsville, Maryland

Steven J. Steindel , Ph.D.
Senior Advisor
Standards and Vocabulary Resource
Information Resources Management Office
Centers for Disease Control and Prevention
Atlanta, GA

Karen Trudel
Director, HIPAA Project Staff
Office of Operations Management
Centers for Medicare and Medicaid Services
Baltimore MD

1284

Staff of the Centers for Disease Control and Prevention, National Center for Health Statistics

Debbie Jackson
Katherine Jones
Marietta Squire
Cynthia Sydney

NCVHS Ad Hoc Work Group on Secondary Uses of Health Data

Simon P. Cohn, M.D., M.P.H., Chair
Justine M. Carr, M.D., Co-Vice Chair
Harry Reynolds, Co-Vice Chair
J. Marc Overhage, M.D., Ph.D.
Mark A. Rothstein, J.D.
William J. Scanlon, Ph.D.
Paul Tang, M.D.
Kevin C. Vigilante, M.D., M.P.H.

Work Group Staff

Kelly Cronin, HHS, Office of the National Coordinator for Health Information Technology
Mary Jo Deering, Ph.D., HHS National Institutes of Health, National Cancer Institute
J. Michael Fitzmaurice, Ph.D., Agency for Healthcare Research and Quality
Erin Grant, Booz-Allen & Hamilton
Morris A. Landau, J.D., M.H.A., L.L.M., HHS, Office of the National Coordinator for Health Information Technology
John Loonsk, M.D., Office of the National Coordinator for Health Information Technology
Kristine Martin-Anderson, Booz-Allen & Hamilton
Steven J. Steindel, Ph.D., HHS Centers for Disease Control and Prevention

Consultant Writer

Margret Amatayakul, MBA, RHIA, CHPS, CPEHR, FHIMSS, Margret\A Consulting, LLC

Appendix B: Testifiers to Ad Hoc Work Group on Uses of Health Data

Karen Adams, Ph.D., National Quality Forum

Elisabeth Belmont, Esq., MaineHealth

Meryl Bloomrosen, M.B.A., RHIA, American Medical Informatics Association

Carmella Bocchino, America's Health Insurance Plans

Cindy Brach, Agency for Healthcare Research and Quality

William Braithwaite, M.D., Ph.D., Health Information Policy Consulting

David Carlisle, M.D., California Office of Statewide Health Planning and Development

Jean Chenoweth, Thomson Healthcare

Deborah Collyar, Group Health Cooperative

Carol Diamond, M.D., M.P.H., Markle Foundation

Richard S. Dick, Ph.D., You Take Control

Howard Dickler, M.D., Association of American Medical Colleges

Linda L. Dimitropoulos, Ph.D., RTI International

Marchelle Djordjevic, American College of Surgeons

Floyd Eisenberg, M.D., M.P.H., Siemens Medical Solutions Health Services

Lynn Etheredge, George Washington University

Sean Flynn, Legal Consultant to the Prescription Project

Jonathan Gold, M.D., MHA, MSC, McKesson Provider Technologies

Joel W. Goldwein, M.D., Elekta, Inc.

Margaret Gunter, Ph.D., RN, HMO Research Network and Lovelace Clinic Foundation/NM RHIO

John Halamka, M.D., CareGroup Health System and Harvard Medical School; Health Information Technology Standards Panel

Assaf Halevy, dbMotion, Inc.

Marcelline R. Harris, Ph.D., RN, Mayo Clinic

Vicki Hohner, M.B.A., Fox Systems, Inc.

Monica Jones, The Information Centre for Health and Social Care, UK

Julie Kaneshiro, Office for Human Research Protection, HHS

Susan Kleimann, Ph.D., Kleimann Consulting Group

Steven E. Labkoff, M.D., FACP, Pfizer Healthcare Informatics

Shirley S. Lady, Blue Cross Blue Shield Association

Leslie Lenert, M.D., Centers for Disease Control and Prevention

John R. Lumpkin, M.D., MPH, Robert Wood Johnson Foundation

Jennifer P. Lundblad, Ph.D., M.B.A., Stratis Health

Janet Marchibroda, eHealth Initiative

Glen Marshall, Siemens Medical Solutions

Sue McAndrew, Office for Civil Rights, HHS

Clement McDonald, M.D., NLM, National Institutes of Health

Julie Murchinson, Manatt Health Solutions

Sharyl J. Nass, Ph.D., Institute of Medicine Privacy Committee

William C. Nugent, M.D., Dartmouth-Hitchcock Medical Center

William J. O'Byrne, New Jersey e-HIT

Wendy E. Patterson, Esq., National Cancer Institute

Deborah Peel, M.D., Patient Privacy Rights Foundation

Kevin Peterson, M.D., M.P.H., University of Minnesota School of Medicine

Steven Posnack, M.H.S., M.S., Office of the National Coordinator for Health IT

Mike Rapp, Centers for Medicare & Medicaid Services

Lori Reed-Fourquet, *e-HealthSign,* LLC

Peter M. Sandman, Ph.D., Risk Communication Consultant

Barbara Siegel, M.S., RHIT, American Health Information Management Association

Sharon L. Sprenger, RHIA, CPHQ, MPA, The Joint Commission

Latanya Sweeney, Ph.D., Carnegie-Mellon University

Sharon F. Terry, M.A., Genetic Alliance

Micky Tripathi, Ph.D., MPP, Massachusetts eHealth Collaborative

Emily Welebob, R.N., M.S., Indiana Health Information Exchange, Inc.

P. Jon White, M.D., Agency for Healthcare Research and Quality

William A. Yasnoff, M.D., Ph.D., Health Record Banking Alliance

Scott Young, M.D., Kaiser Permanente

Appendix C: Taxonomy/Glossary of Terms

This taxonomy, with a glossary of terms (*under development*), identifies and defines terms used by testifiers (and in collateral documents) in discussion of uses of health data. Its purpose is to provide guidance to the reader of this report as well as to inform the development of its recommendations. The structure of the Taxonomy/Glossary of Terms is generally consistent with the "Secondary Uses and Re-uses of Healthcare Data: Taxonomy for Policy Formulation and Planning" (a.k.a., AMIA Taxonomy) developed by the American Medical Informatics Association (AMIA). However, there are both similarities and differences between the two documents that are important to note:

- The NCVHS Taxonomy/Glossary of Terms is intended to inform the recommendations included herein and to help provide guidance in determining suitable data stewardship approaches for various uses of health data by the entity having jurisdiction over the use.

- The AMIA taxonomy is intended to be used as a "resource in developing plans and policies related to secondary uses of healthcare data." The AMIA taxonomy attempts to provide a categorization of health data uses that could be described by various attributes of the uses and therefore relate policy statements to the particular use.

- Neither the AMIA Taxonomy nor the NCVHS framework attempts to be inclusive of all categories or classes of uses or users of health data nor all attributes of the uses of health data for policy purposes.

- The NCVHS Taxonomy/Glossary of Terms includes annotated definitions to guide the reader of the report as well as to promote adoption of standard terminology associated with uses of health data.

Taxonomy/Glossary of Terms Structure

Needs description

Taxonomy and Terms

<u>Terms Used to Describe Status of Information</u>
Individually identifiable health information (IIHI), as defined by HIPAA
Protected health information (PHI), as defined by HIPAA
Personal health information, as commonly used

<u>Terms Used to Describe Oversight of IIHI</u>
Covered entity compliance with HIPAA
Business associate contract/agreement

Agent of business associate
Researcher compliance with regulations
Data use agreement, as defined by HIPAA
“HIPAA compliant” (when used by vendors)
Data Ownership
Data stewardship

Terms Used to Describe Identity Protection (of Individual Patient/Clinician; Entity)

De-Identification, as defined by HIPAA using statistical and scientific principles and methods for rendering information not individually identifiable
De-Identification, as defined by HIPAA safe harbor
Limited Data Set (HIPAA for Public Health, Research, or Health Care Operations)
Non-identifiable/un-identifiable
Anonymization (Public Health)
Pseudonymization (Public Health)
Irreversible Pseudonymization
Linked data with protected key
Re-identifiable
Aggregation (Quality)
Information vs. Data (Markle)
Masking
Encryption
One-way Hash

Terms Used to Describe Permission to Access/Use/Disclose

Authorization (HIPAA Privacy)
Authorization (HIPAA Security)
Consent (HIPAA permits but does not require)
Consent (Common Rule required for Research)
Consent (Informed for Procedures)
Opt In
Opt Out (also HIPAA Opportunity to Agree or Object; Right Request for Restrictions)
De-authorization
IRB approval; IRB waiver

Terms Used to Describe Uses of Data

Primary
Secondary (AMIA Taxonomy Sources of Secondary Data; IOM [1991] Uses and Users)
Tertiary, Quaternary
Non-Clinical Use

Terms Used to Describe Transparency

HIPAA Notice of Privacy Practices (often confused with consent)

Terms Used to Describe Accountability

Sanctions

Civil Penalties

Criminal Penalties

Terms used to Describe Health Information Repositories

Medical record

Health record

Legal health record (AHIMA)

Electronic health record

Personal health record

Continuity of care record; (ASTM CCR) + clinical document architecture (HL7 CDA) = continuity of care document (CCD)

Clinical data repository

Clinical data warehouse

Terms Used to Describe Exchange of Health Information

ONC:

Health information exchange

Nationwide health information network

Nationwide health information network health information exchange (NHIE)

Health information service provider (HSP)

NCVHS:

National health information infrastructure

Data access (in some cases view only; in other cases obtaining an image of data; in still other cases obtaining the data in processable form)

Data sharing

Data use

Data disclosure

Data request

Terms Used to Describe Circumstances that Raise Policy Issues (AMIA)/Trust (NCVHS)

Financial Gain from Use

Quality

The Institute of Medicine (IOM) report on Performance Measurement: Accelerating Improvement (2006) defines *quality* as “the degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge.” This report also describes *performance measures for quality* as inclusive of patient perspectives on care, clinical quality, and patient outcomes.